Reliability Engineering and System Safety 208 (2021) 107392

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Supervised dynamic probabilistic risk assessment of complex systems, part 2: Application to risk-informed decision making, practice and results

Tarannom Parhizkar [a,*], Ingrid Bouwer Utne [a], Jan Erik Vinnem [a], Ali Mosleh [b,c]

[a] Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[b] The B. John Garrick Institute for the Risk Sciences, University of California, Los Angeles, LA, USA
[c] Department of Materials Science & Engineering, University of California, Los Angeles, LA, USA

ARTICLE INFO

Keywords:
Dynamic probabilistic risk assessment
Supervised algorithms
Dynamic positioning system
Cognitive models
Risk-based decision making
Emergency situations

ABSTRACT

One challenge that has received attention in maritime industry is assessing the risk level of dynamic positioning (DP) systems in emergency situations. Statistics from recent years have shown that the risk level of some DP operations is above the industry's risk criteria. Operators have a significant impact on incidents' consequences by making responsive decisions. In emergencies, one is afforded little time to make a decision. Available risk models are not efficient enough to provide systems' risk level in a short period of time.

In this study, the application of a new supervised methodology to assist decision making in emergencies is proposed. This method significantly reduces the processing and execution time of a system's probabilistic risk assessment models. In this methodology, the most probable failure scenarios are generated using an optimization model. The objective of the optimization model in this study is to find scenarios with the highest occurrence probabilities. The constraints are a system's dynamic simulation and its risk model. The proposed method is applied to three incidents that occurred in the Norwegian offshore sector in previous years. The results show that the model can predict the most probable scenarios with an acceptable accuracy in a very short time.

1. Introduction

During the early development of dynamic positioning (DP) systems, researchers and engineers focused on a number of important aspects, including technology development [1,2] and regulation [3]. Moreover, in recent years DP operational reliability and risk assessment have gained significant traction.

In [4], the quantitative reliability of offshore multi-megawatt capacity diesel electric DP systems is assessed based on contemporary components technology, revealing that DP classes 1, 2, and 3[1] have mean time to fail periods of 0.3, 2.1 and 2.5 years, respectively. These results may be used for the reliability-centered design and maintenance planning of multi-megawatt capacity DP systems. Moreover, Chen et al. [5] have developed a safety model based on the barrier concept for DP drilling operations. Three main barrier functions (barrier functions to prevent loss of position, to arrest vessel movement, and to prevent loss of well integrity) are considered in the modeling. Analyses of each barrier function identify the associated barrier elements, and the authors propose recommendations to strengthen each barrier element.

In [6] and [7], Man, Technology and Organization (MTO) analysis is applied to investigate the cause and barrier failures of nine reported accidents/incidents of DP shuttle tankers occurring over a 16-year period (2000–2015). The results show that the majority of these accidents are caused by a combination of technical, human, and organizational failures. In addition, human error is found to constitute one of the major factors involved in these incidents.

The Institute for Energy Technology has developed a method called Petro-Human Reliability Analysis (HRA) to analyze human actions as barriers in major accidents in the petroleum industry. In [8], this method is applied to a dynamic positioning drilling operation, and the risk level is calculated for a drive-off scenario. In addition, in this report the personal shaping factors of operators are identified, and the related quantities are presented. The study notes that personal shaping factors could be used to quantify human errors based on the Standardized Plant

* Corresponding author: Department of Marine Technology, NTNU, 7491 Trondheim, Norway.
E-mail addresses: tarannom.parhizkar@ntnu.no, parhizkar.t@gmail.com (T. Parhizkar).

[1] Based on international maritime organization publication, the classification societies have issued rules for dynamic positioned vessels described as Class 1, Class 2 and Class 3.Equipment Class 1 has no redundancy. Loss of position may occur in the event of a single fault.Equipment Class 2 has redundancy so that no single fault in an active system will cause the system to fail.Equipment Class 3 also has to withstand fire or flood in any one compartment without the system failing.

https://doi.org/10.1016/j.ress.2020.107392
Received 20 March 2020; Received in revised form 21 October 2020; Accepted 27 November 2020
Available online 4 December 2020

Analysis Risk-Human Reliability Analysis (SPAR-H) method.

In Dong et al. [9], generic scenarios of position loss during the operation phase of DPs are identified. The results show that position loss normally involves complex human-machine interactions. According to the study's findings, the time aspect plays a significant role in developing an online risk model for DP operations. Hogenboom et al. [10] have highlighted the importance of considering human operator and human reliability in the design and operation of DP systems. In this paper, a functional model of the DP system is presented, and the current function allocation of control and its impact on an operator's situation awareness and performance are discussed. It is concluded that the visualization of operational risk could enhance operator performance and reliability.

According to the reviewed literature, human error has a remarkable impact on DP incidents, especially in emergency situations. Having a clear picture of the risk level of decision scenarios could help operators to make better decisions [11–13], and consequently ensure safer DP operations. In this study, a dynamic probabilistic risk assessment (DPRA) methodology for DP systems is developed. This methodology considers the interactions of MTO over time in an emergency situation, and provides the risk level of the system accordingly.

The dynamic probabilistic risk assessment method is a powerful tool in assessing the risk level of complex systems [14] such as DPs. DPRA refers to an emerging class of PRA methods that generate risk scenarios through model-based simulations of systems such as DPs and their operators' responses to accident initiators [15]. The dynamic PRA approach offers several advantages over the conventional approaches currently used by the marine industry worldwide. These advantages include: (1) time-dependent prediction of operator error-forcing contexts; (2) better representation of position control success criteria; and (3) considerable reduction in results' analyst-to-analyst variability. In [16], a dynamic risk assessment framework for DPs is proposed. The framework supports the decision-making of operators with providing failure probability of different possible decision scenarios. This framework considers technical, human and organizational factors in the modeling process. The input data including frequencies and failure probabilities are gathered from the International Marine Contractors Association (IMCA) annual incident reports on DP systems from 2004 to 2015 (IMCA, 2017). The framework is applied to a loss of position incident that occurred on a mobile offshore drilling unit.

With the growth in dynamic systems and the complexity of the interactions between hardware and humans, it is extremely difficult to enumerate risky scenarios using conventional DPRA methods [17,18]. As the complexity of the system increases, system behavior would be more uncertain [19]. In a more uncertain environment, the number of possible failure scenarios increases significantly. In the DPRA conventional methods, all these scenarios should be analyzed, and system risk level is calculated accordingly. Therefore, increasing the number of possible scenarios due to uncertainty, increases the execution time of the conventional DPRA methods dramatically. The effect of system complexity on DPRA methods is explained in more detail in [17] and [18].

In our study, presented in the accompanying article (Part 1) [20], a supervised dynamic probabilistic risk assessment methodology is proposed. In this methodology, a new investigation strategy is employed that searches for the failure scenarios of interest, instead of analyzing all possible failure scenarios. The scenarios of interest could be the scenarios with high risk level or the most probable scenarios. The modeler could define the desirable scenarios based on the goal and scope of the study.

In the proposed supervised DPRA method, optimization algorithms are explicitly used to guide the DPRA model to find and analyze scenarios of interest (without solving all possible failure scenarios). In the accompanying article (Part 1), a comparison between execution time of a conventional DPRA (dynamic event sequence diagrams) and the supervised (optimization based) DPRA methods is performed. Results show that the execution time of the supervised optimization based DPRA method is significantly lower than the conventional method. In the current study, the application of this method on risk-informed decision-making in DP systems is presented. The main contributions can be summarized as follows:

- A supervised DPRA methodology for DP operations in emergencies is developed (Section 3).
- Human and organizational factors are considered in the DPRA (Section 3.4).
- Three DP incidents are considered as case studies, and the results, including the most probable failure scenarios and risk levels, are evaluated (Sections 4.1, 5.1, and 6.1).
- Sensitivity analysis on operational and environmental characteristics are performed, and the most significant parameter within DP incidents is identified (Sections 4.2, 5.2, 6.2, and 7).

The paper is organized as follows: a brief overview of the methodology developed is introduced in Section 2. Details of the methodology are presented in Section 3. In Sections 4, 5 and 6, three DP incidents are modeled, the results of which are presented accordingly. In Section 7, the results of three case studies are summarized and analyzed. In Section 8, the usefulness and drawbacks of the proposed methodology are discussed. Finally, the conclusions and the contributions of this study are presented in Section 9.

2. General methodology and concept

Fig. 1 presents a flow diagram of the dynamic probabilistic risk assessment based on supervised learning algorithms developed in the accompanying article (Part 1), [20]. As illustrated in Fig. 1, the measurable data from a DP system are model inputs; these inputs might constitute alarms, operational or environmental sensor data. These data enter supervised failure scenario generation module. In this module, desired failure scenarios are generated using an optimization model. The optimization model is developed in five consequences steps, which are explained in the following sections. Based on these steps, a general risk assessment model for the DP system under study is developed. The risk assessment model consists of pre-calculated offline information, which are not required to be updated in emergency situations. This information includes characteristic of the components that could be considered constant in an emergency (short term), e.g., engine efficiency, operators training level, etc.

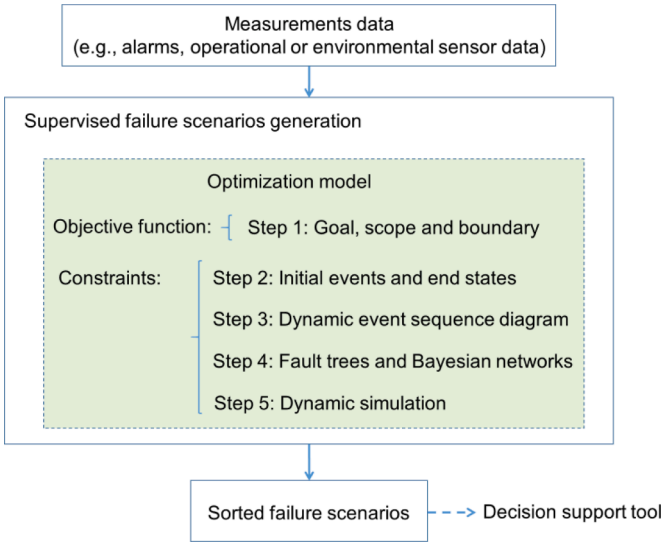

Fig. 1. Flow diagram of the supervised probabilistic risk assessment.

In real-time, the model is updated based on the measurement data and the output is generated. The output of the module is a set of failure scenarios which are sorted based on a metric such as failure probability or significance of failure consequences. The metric should be defined in the optimization model by the modeler. Based on the defined metric, failure scenarios are sorted and reported to the operators. This information could assist operators to make better decisions in emergency situations. This methodology could be applied to any type of DP systems.

The supervised failure scenario generation utilizes an optimization model to build desired scenarios such as success scenarios, failure scenarios or scenarios with a high impact. The generation of failure scenarios is of interest in this study, i.e., the proposed optimization model helps to generate failure scenarios in a DP system, without generating all other possible scenarios. As a result, the execution time is significantly improved, and the probabilistic risk level can be calculated in a very short execution time. One of the main applications of this method is in emergency situations in which operators have limited time to make decision. This method can generate a risk level of alternative operating scenarios in a very short execution time.

An optimization model consists of an objective function and a number of constraints. The objective function is the real-valued function whose value is to be either minimized or maximized over the set of feasible alternatives. Moreover, a constraint is a condition of the optimization problem that the solution must satisfy. There are several types of constraints, including inequality, equality and integer constraints. The set of candidate solutions that satisfies all constraints is called the feasible set. In order to find the optimal solution among the feasible set, an optimization algorithm should be executed. Multiple solution algorithms have been proposed for optimization problems. According to the performance of the solution algorithm, the best suitable algorithm should be selected for the system under study. Further information on optimization models and solution algorithms could be found in [21,22].

3. Implementation of the methodology

In this section, the steps of implementing the supervised failure scenario generation on a complex system are presented. As mentioned, a DP system is an example of a complex system. It represents a computer-controlled system to automatically maintain a vessel's position and heading by using its own components [16]. A DP system consist of computer, propulsion, reference, power and control systems. The operating and environmental condition data are collected using reference systems. These data are analyzed in the DP computer and action signals are sent to propulsion and control systems to maintain the vessel position and heading. All these components should work properly to be able to control the vessel. Failure of one component could result in the failure of the DP system. The crew have an important role in the case of components' failure. They could detect and diagnose faulty components, and make a decision to recover the DP system or control the vessel manually based on the system and environmental conditions.

At each step presented in this section, a general modeling strategy is followed by the implementation of the strategy in a DP system.

The decision-making process consists of four main steps, including detection, diagnosis, decision making and execution that interacts with the DP system. In this study, the interaction between human operator and DP components are models; and the risk of decision making in emergencies is presented and discussed. In the following sub-sections, the steps of the modeling, presented in Fig. 1, are followed and the proposed methodology is applied to the case studies.

3.1. Step 1: goal, scope and boundary

This study seeks to generate failure scenarios of DP systems in emergency situations. A DP emergency situation is a condition in which a system failure results in an inability to maintain position or heading control [23]. A system boundary comprises environmental and technical factors that affect an operator's decision making and action process. Decisions are made according to detection and diagnosis phases, with actions taken accordingly. Actions may be taken either automatically or manually. In automatic mode, a DP system is utilized to take the action and to try to maintain the vessel's position, whereas in manual mode an operator controls the vessel's position and heading [24].

3.2. Step 2: initial events and end states

Initial events may be any abnormal condition of the vessel that leads to a failure to maintain its position. End states can be OK status (maintain position), or failure status (loss of position, collision, mechanical damage, etc.).

3.3. Step 3: dynamic event sequence diagram

The event sequence diagram method is used in risk assessment problems [25,26]. Dynamic event sequence diagrams (DESDs) are extended versions of event sequence diagrams (ESDs) that could be used as a DPRA methodology. DESDs can consider system dynamic behavior in the modeling process [27,28]. They can be used in combination with dynamic methodology computational algorithms, which seek to solve the underlying probabilistic dynamics behavior of complex systems over time. The probability of events in DESDs could be quantified based on different probabilistic methods, such as Bayesian networks and fault trees, which are discussed in the following sections.

There are different considerations on the development of DESDs, e.g., timestamps are implicit with BNs but usually explicit with DESDs models. More details on DESD methodology could be found in [28–30].

Fig. 2 presents a DESD for decision making processes of DP systems in emergency situations. This diagram contains all the possible event sequences that could occur after an initial event under different operational, human, and environmental conditions.

The first layer presents detection alternatives. Alarms represent the most common means of incident detection; however, sometimes operators perform other methods, including checking the vessel's position or making other visual detections such as of the engine room or weather. The probability of alarm detection depends on an alarm system's health status as well as operator's personal shaping factors. Moreover, the occurrence probability of performing a "position check" or "other visual detection" is contingent on an operator's personal shaping factors. For instance, it is more probable that an experienced operator performs "other visual detections" than an entry-level operator. The occurrence probabilities of these three detection processes are a function of an operator's behavioral factors, and can be calculated using the Bayesian networks (BNs) presented in Section 3-4. In order to be rendered more practical, an operator's measurable behavioral factors, including fitness for duty, stress and training level, are selected as BN inputs. These parameters can be updated in real time in a DP vessel.

The next layer presented in DESD is the diagnosis phase. In this layer, operators try to figure out the status of the system and control the situation in order to return the system to its normal operation. In this stage, if there is enough time (defined in [8]), operators check DP components in order to identify the main causes of the incident as well as the consequences (drift off, drive off and potential incidents). Alternatively, operators attempt to control the situation using the available information from the detection layer and DP screens. In addition to available time, the probability of performing components diagnosis depends on detection accuracy. If the detection accuracy is high, components diagnosis is unnecessary, as sufficient information has already been attained from the detection layer. Table 1 presents the assumed rules based on expert knowledge for connection between the detection layer and the diagnosis events (control situation, components diagnosis) as a function of time and detection accuracy. The limited/enough time and detection accuracy levels could be determined by experts. In this study, the limited and enough times are defined based on [8] and a high

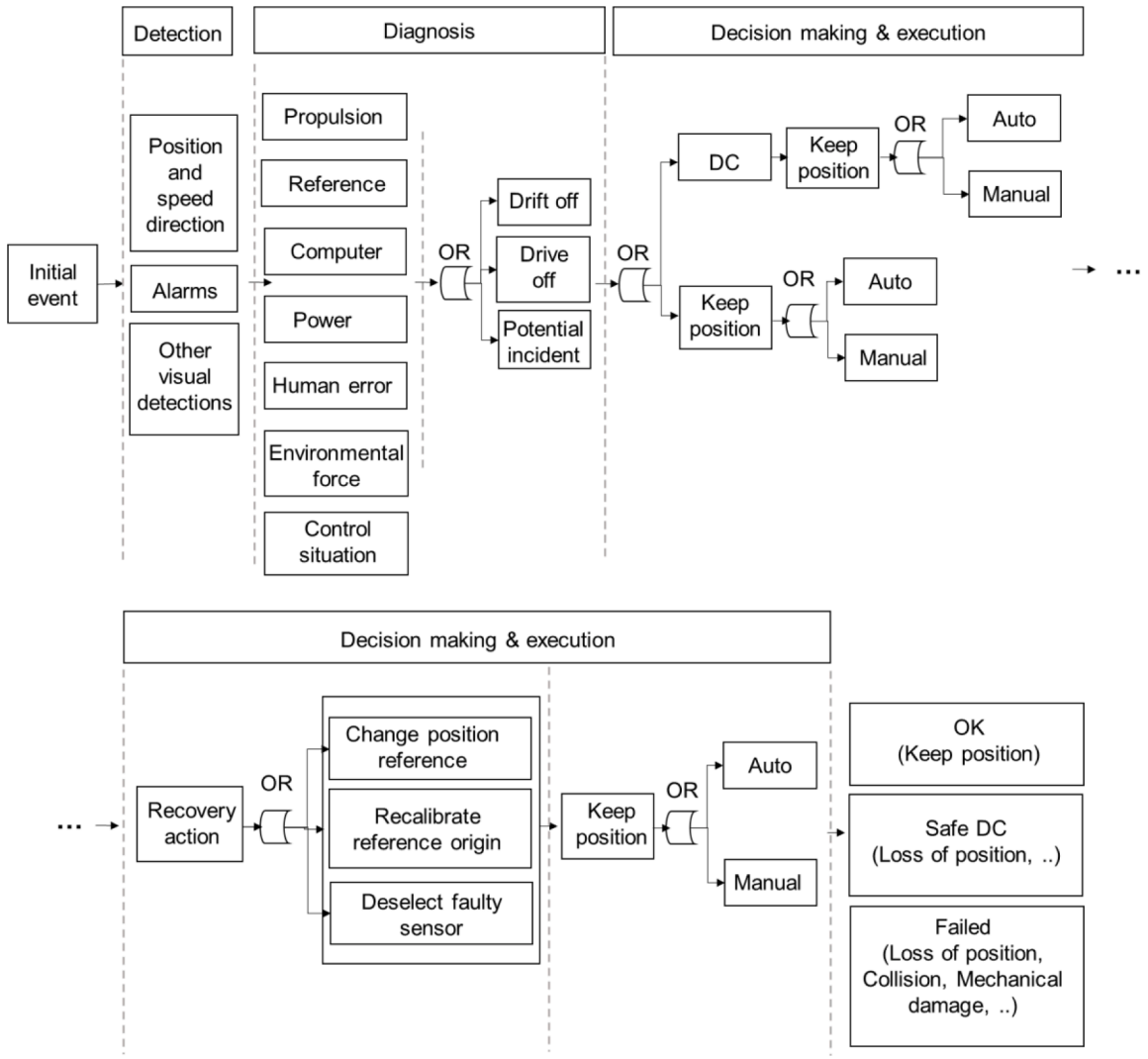

Fig. 2. Dynamic event sequence diagram of DP systems.

Table 1
Selection rules of connection alternatives between detection and diagnosis layers.

Time	Detection accuracy	Connection
Limited	High/Low	Connection to control situation
Enough	High	Connection to control situation
Enough	Low	Connection to components diagnosis

accuracy level is set to 0.95 and above.

If components diagnosis is selected, the probabilities can be calculated using the associated fault trees (FTs) presented in Section 3.4. In addition, the probabilities of components selection are equal, unless a clear alarm from one component is detected. In such a case, the probability of selecting a related component is higher.

Following components diagnosis, the possible consequences should be identified. In this step, the probabilities of consequences including drive off, drift off, potential incident and dismiss alarm are calculated. The probabilities of drive off, drift off and potential incident depend on components status and are calculated according to The International Marine Contractors Association (IMCA) reports from 2004 to 2015 [31]. If there is no fault in the components and environmental conditions, dismiss alarm is selected as an active event in the DESD.

As mentioned, the other step in the diagnosis process is "control situation". The probability of this event can be calculated using the BN presented in Section 3.4. The next layer of the DESD is decision making and execution. In this layer, operators decide to stop the vessel (disconnection) or try to keep position. In either case, operators can select manual or automatic mode to perform the task. Selecting the task (disconnection or keep position) and mode (automatic or manual) depends on multiple factors, including standards, an operator's personal shaping factors (PSFs), components status, available time and so forth.

For instance, in DP drilling units, specific operating guidelines (WSOG) are used to define the actions that should be taken by a dynamic positioning operator in the event of certain changes to the DP units' capability [32]. Whenever a system passes the yellow region (defined in WSOG) and enters the red region (defined in WSOG), the operator must perform disconnection. As a result, if the vessel operates in a "red situation", the probability of selecting disconnection mode is higher than keeping position. In "green & yellow situations", selecting the keep position branch has a higher probability.

Moreover, based on the DP's functionality, it is assumed that the disconnection or keep position modes are performed automatically unless a failure in reference and/or computer system occurs. The manual mode selection rules are defined based on expert knowledge and presented in Table 2. For all other conditions, the probability of manual or automatic modes being selected can be considered equal.

The probabilities of automatic/manual disconnection or keep position performance can be calculated using the fault trees and Bayesian

Table 2
Selection rules of automatic or manual modes.

Component	Status	Connection
Reference system	Failed	Manual mode
Computer	Failed	Manual mode

networks presented in Section 3.4.

One of the other layers in decision making and execution is performing recovery actions. It is assumed that the probability of performing a recovery action depends on the time available. In situations with limited time, no recovery actions are performed. However, if there is sufficient time, recovery actions can be performed. According to expert knowledge, the recovery actions of DP systems in emergency situation are limited to seven scenarios, which are presented in Table 3. The required execution times of each recovery scenario are gathered based on expert knowledge as well, and are shown in the final column of Table 3.

3.4. Step 4: fault trees and Bayesian networks

The failure probability of each event presented in the DESD (Fig. 2) can be calculated using the related fault trees and Bayesian networks presented in [16]. The fault trees of the propulsion, reference, power, automatic control and manual control systems are presented in [16].

The remainder of the events presented in the DESD are human-related. The failure probabilities of these events depend on the type of action performed. In [16], the Bayesian networks of detection, diagnosis, decision making, and execution actions are constructed and quantified. Figs. 3, 4 and 5 present the Bayesian networks presented in this study for detection, diagnosis, decision making and execution actions, respectively.

The quantification process of the presented Bayesian networks is discussed in detail in [33]. It should be noted that in this study, the parent nodes are modified; and nodes that can be quantified using sensors or questionnaires with operators are considered as child nodes. These nodes include an operator's fitness for duty, stress and training level. The rest of the child nodes, such as ergonomics and work processes, are not included in this study. Eliminating these nodes will result in a more realistic and certain model. In the abstracted model, the status of all parent nodes can be updated based on the real data from sensors/questionnaires, i.e., there is no need to assume the value of unknown inputs. Adding assumption on unknown input data results in model uncertainty, that is eliminated in the abstracted model.

3.5. Step 5: DP system simulation

As mentioned in Section 3.3, some of the connection probabilities are dependent on the time available. For instance, if there is enough time (defined in [8]), components diagnosis can be performed, or recovery actions can be taken. In this study, a dynamic simulator is utilized to calculate the remaining available time, considering operation and environmental conditions [34]. This time depends on components status

Table 3
Recovery actions of each component and related timelines.

Component	Recovery actions	Required execution time
Reference	1- Change position reference	3–5 s
	2- Recalibrate reference origin	50–60 s
	3- Deselect faulty sensor	3–5 s
Control	4- Reference system recovery	3–60s
	5- Tuning software	30 s
Power	6- Start new generator and connect it	30–60 s
Propulsion	7- Safe start of equipment on alternative switchboard	30–60 s

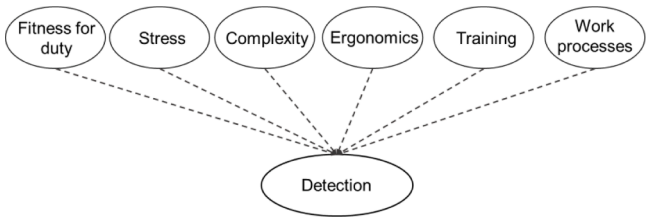

Fig. 3. Bayesian network of detection probability [16].

(engines, thrusters, control system, etc.), environmental conditions (wind force and direction, wave force and direction, etc.), and DP type. For instance, the remaining available time in DP drilling units is equal to the minimum required time that the vessel reaches the red limit, as presented in Fig. 6. The remaining available time in DP supply vessels is equal to the minimum required time that collision occurs between the DP supply vessel and a floating storage and offloading vessel (FSO). This time is contingent on DP components status and environmental conditions. The remaining available time can be defined for other types of DP systems based on DP operating functions. This definition can be used in DP dynamic simulators to formulate the calculation of the remaining available time.

Fig. 7 illustrates a sample of the outputs of a dynamic simulator. As can be seen, the operational and environmental conditions of the DP system, including wave, current power system, control system and propulsion system characteristics, are taken as inputs [36]. Using dynamic simulation, the position and the velocity of the DP system over time are calculated. In this example, it is assumed that the DP vessel is 20 m away from the red limit. The dashed red line in the reference position figure presented in Fig. 7 shows the time it takes to move 20 m into the red area, which is about 900 s.

3.6. Optimization model

An optimization model is used to generate desired failure scenarios, without exploring all possible scenarios after an incident. The first step in developing an optimization model is to define an objective function. The objective function determines the scenarios that should be generated, and it is defined based on the scope/goals of the study.

The objective of this study is to find the most probable failure scenario, and is presented in Eq. (1)

$$Max \sum_{j=1}^{m}\sum_{i=1}^{n}(p_{ij}\times x_{ij}) + \sum_{k=1}^{r}\sum_{j=1}^{o}\sum_{i=1}^{l}(p_{ijk}\times x_{ijk}) \quad (1)$$

where the first term presents the occurrence probability of each event in each layer of the event sequence diagram. n is the number of events in each layer, and m is the number of total layers, which is equal to 8, as presented in Fig. 2. The second term presents the connection probability between events in two neighboring layers. l is the number of events in the initial layer, and 0 is the number of events in the secondary layer. r is the total number of possible connections between layers. p_i presents the probability of an event or connection, while x_i is a binary variable {1,0} that indicates the existence and/or non-existence of an event or connection, e.g., an event/connection with x_i=1 represents the existence of the event/connection in the most probable scenario.

The probability of events and connections is a function of the operational and environmental conditions in question. Based on the ESD, FTs, BNs (Section 3.4) and the dynamic simulation model (Section 3.7) developed and presented in the previous section, these functions are quantified and presented as optimization model constraints, i.e., all the governing principle rules of the ESD, FTs, BNs and the dynamic simulation model are considered as optimization model constraints.

The objective function and constraints of this optimization model are nonlinear and decision variables are integer. Therefore, mixed-integer

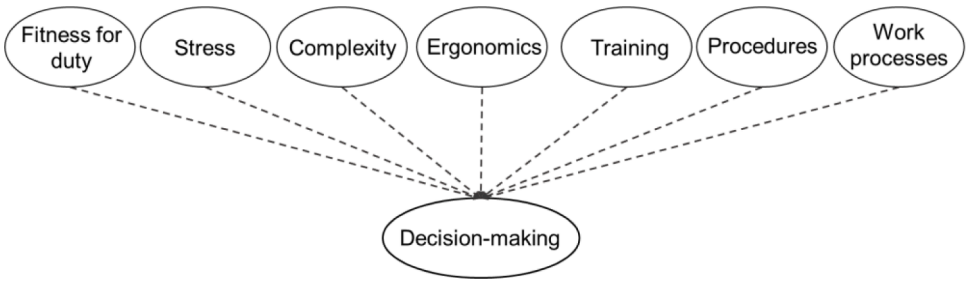

Fig. 4. Bayesian network of diagnosis and decision-making probabilities [16].

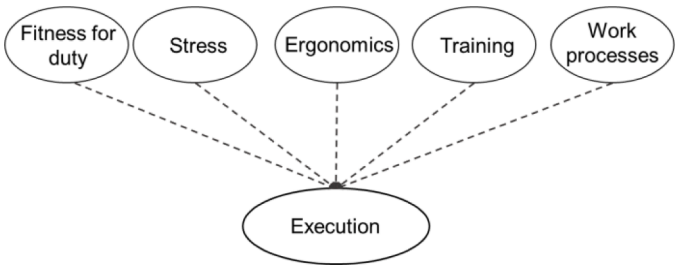

Fig. 5. Bayesian network of execution probability [16].

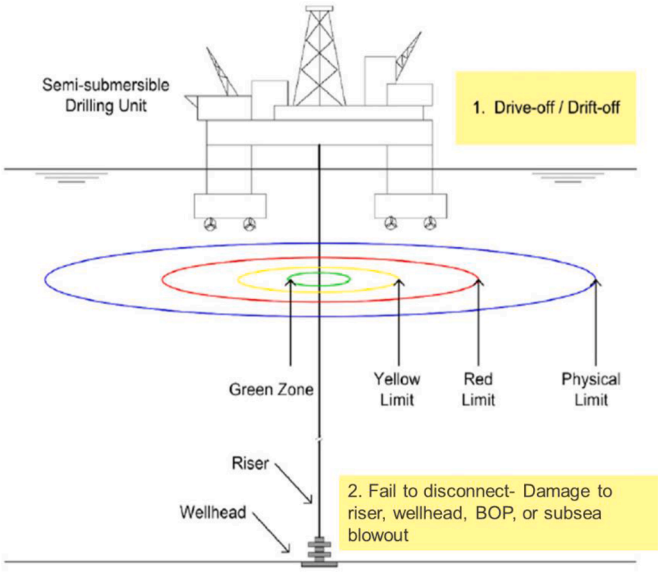

Fig. 6. DP drilling operation zones [35].

nonlinear programming (MINLP) methods can be utilized to find the optimal solution. Multiple solution algorithms have been proposed for MINLP problems [37]. According to the performance of the solution algorithm, a modified particle swarm optimization (PSO) algorithm [38] is selected for the system under study.

3.7. Probabilistic risk assessment

The outputs of the optimization model are the optimal decision variable matrix X, and its probability value. The X matrix represents the most probable failure scenario with binary values. For instance, the following matrix is an example of an optimal scenario. Each column is a layer presented in the ESD, i.e., the first column is the detection layer, the second and third columns are diagnosis layers, the fourth, fifth and sixth columns are the decision making and action taking layers, and the last column is the end state layer. These layers are presented and separated with dashed lines in Fig. 2.

$$X_{Opt} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

According to this example, at the detection layer (first column), the alarm is detected (the second element is equal to one and the rest are zero). Then, at the second column, diagnosis on the computer system is performed (X_{32}=1 and the rest of the elements are equal to zero). The rest of the columns can be translated accordingly (element equal to 1 shows the existence of the related event in the ESD).

Another output of the optimization model is the probability of the optimal scenario. For instance, $p(X_{opt})$ may be equal to 0.01. This means that the probability of the optimal scenario is equal to 0.01.

After finding the most probable scenario, this scenario is eliminated, and the optimization model is run again to find the second most probable scenario. This process is repeated until the least desired scenario is generated.

In the following section, the model is applied to three incidents as case studies. The inputs of the model are gathered from the investigation reports of each incident. The model is run, and the most probable scenarios are generated for each case study accordingly.

4. Application 1: collision of a DP shuttle tanker on November 13, 2006

4.1. Incident summary and failure scenario generation

On November 13, 2006, a DP shuttle tanker touched an FSO as it started its loading operation. The shuttle tanker sustained some damage above the waterline in the bow area. The FSO suffered damage to its stern and to some equipment in the after part of the poop deck. According to the established investigation report, the DP shuttle tanker was operating in automatic positioning mode and had just received and secured the mooring hawser. As the bow crew was in the process of preparing the loading hose transfer, a blackout of the starboard main switch board (MSWB) occurred. The blackout caused a loss of starboard main propulsion as well as a loss of side thrusters numbers 2 and 4, as these were powered by the said MSWB.

Unexpectedly, side thrusters' numbers 1 and 3 also stopped due to a lack of power. As per DP class 2 requirements, these thrusters are powered by the port MSWB, for which the main power is completely separated from the starboard MSWB, and thus its main power was not affected by the blackout. With only the port main propeller and rudder available on the DP, the vessel remained in DP automatic positioning mode. The DP system was not capable of maintaining or controlling its position with only one rudder and one propeller. About four minutes

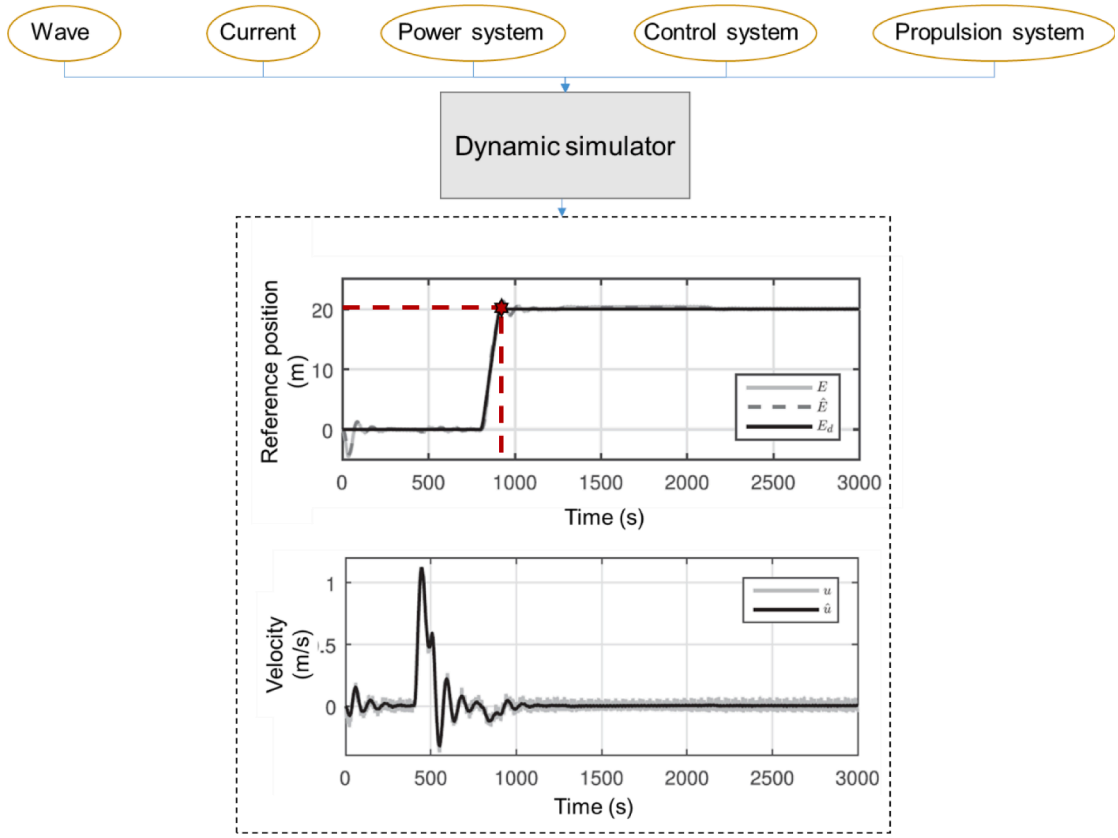

Fig. 7. A sample of dynamic simulator output.

later, the shuttle tanker hit the FSO with approximately 2.4 knots [39]. The impact caused visual damage to both vessels, but no physical injuries to personnel. The sequence of events is highlighted in the dynamic event sequence diagram illustrated in Fig. 8. The presented DESD is developed based on the general DESD of DP system (Fig. 2)

The supervised DPRA model is applied to this case study, and failure scenarios are generated accordingly. The inputs of the model are derived from the investigation report of this incident [39], and are presented as follows.

- Blackout has occurred.
- The operator has enough fitness for duty and training, and the stress level is normal.
- There is not enough time and the DP vessel is in an emergency situation.
- The environmental conditions including wind and waves (force and directions) are in normal conditions.
- The reference and computer systems work properly.
- The propulsion system including thrusters has failed.

Based on these inputs, the model is run, and all failure scenarios (271 scenarios) are generated. Failure of each event presented in Fig. 8 could result in a failure scenario. All possible combinations of event sequences

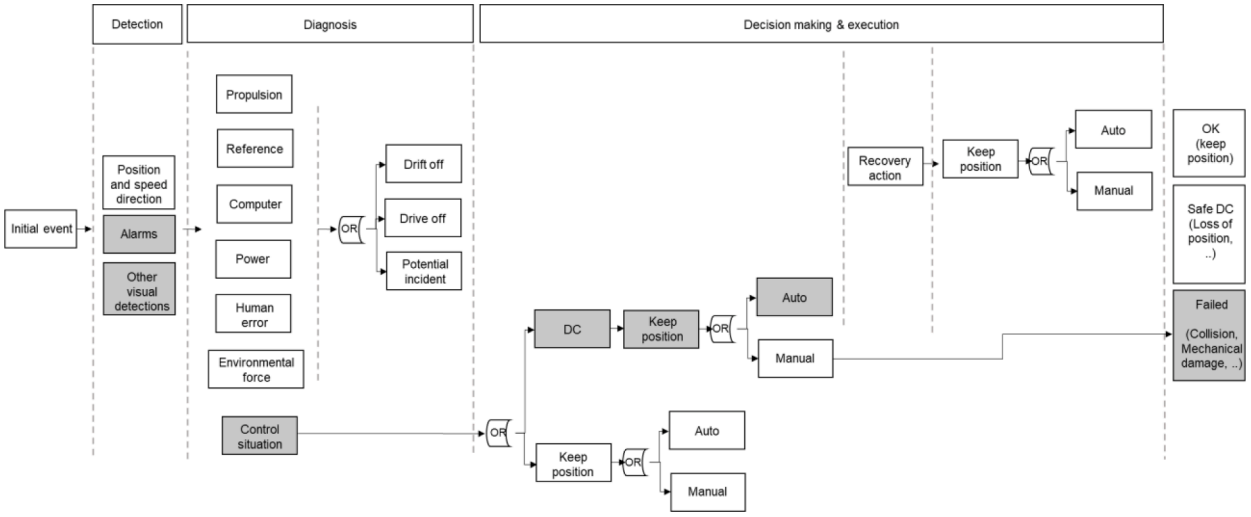

Fig. 8. Dynamic event sequence diagram of the DP shuttle tanker collision.

with a failed end state (last event) are equal to 271 scenarios. In Table 4, failure of each event that could result in generating a failure scenario is presented.

The probability of failure of the presented events in Table 4, could be calculated using BN/FTs presented in Sections 3.3 and 3.4.

Table 5 presents most probable failure scenarios of the DP shuttle tanker collision. The failure scenarios are different branches of the event sequence diagram. The scenarios cannot occur at the same time, so they are mutually exclusive. The probability of system failure is equal to the sum of all failure scenarios probabilities, which is 0.726. The generated scenarios are sorted based on the failure probability, and the most probable scenarios are presented in Table 5.

As can be seen, the scenario that occurred and is presented in the investigation report, presented in the beginning of this section, was the second most probable scenario out of 271 possible failure scenarios. In addition, according to the second and third most probable scenarios, automatic disconnection was more likely to fail than manual, mainly because the DP components (thrusters, etc.) did not work properly. As a result, the failure probability of automatic modes may be deemed higher. However, after recovery actions, DP components work properly. Therefore, manual keep positions are more likely to fail than automatic mode, as presented in the table.

Another point that can be inferred from the table is that two of the recovery scenarios (start of equipment on alternative switchboard and start new generator) are more likely to be performed in order to return power to the system. However, due to the lack of time, the recovery actions may fail.

4.2. Sensitivity analysis

In the following sub-sections, a number of operation and environmental conditions at the time of the incident are altered to evaluate their impacts on the output, i.e., most probable failure scenarios and system failure probability.

4.2.1. Faulty position reference system

The position reference systems are to comply with the relevant requirements for the mandatory classification notations of the vessel for electrical, mechanical, and hydraulic components and subsystems [40]. The accuracy and the limitations of the position references used are to be adequate for the specific task in which the vessel is engaged. In this section, it is assumed that the position reference system was faulty and provided inaccurate data regarding the incident. It is assumed that the faulty reference system has a failure probability of 0.9. This failure probability is used in the "reference" event in the first layer of diagnosis process, presented in Fig. 8. Moreover, it is assumed that the inaccurate data from reference system affect diagnosis process probability (Bayesian network presented in Fig. 4), and the failure probability of diagnosis increases by 30%. Table 6 presents the most probable failure scenarios in this situation.

The overall failure probability in this scenario increases slightly and is equal to 0.728. The reason is that, success or failure of the reference system, while the power system is not working, would not affect the overall failure probability significantly. In a lack of power system, the main engine and the thrusters cannot operate, so having a healthy or faulty reference system would not significantly affect the overall functioning of the DP system. Another point that can be inferred from Table 6 is that in addition to the recovery of the power system, the recovery of the reference system is presented in the most probable scenarios.

4.2.2. Sufficient time

In this section, it is assumed that there is enough time to make a decision and to take action. In other words, it is assumed that the DP vessel is sufficiently far from the FSO, and that a collision between the vessel and the FSO would not happen in a short time. According to PetroHRA [8], sufficient time means that there is enough time to undertake the task, and the operator(s) only experiences a low degree of time pressure or need to speed up in order to complete the task. Table 7 presents the most probable failure scenarios, assuming that there is enough time to undertake tasks after the initial event, i.e., alarm detection.

The overall failure probability in this scenario decreases significantly and is equal to 0.451. Moreover, the rank of most probable scenarios is altered. With enough time, it is more likely that the operator controls the situation, and the scenario of failure in this situation drops from the first to the third level. Another point is that the failure of the recovery action is less probable in comparison to the results presented for the real case with limited available time. This indicates the impact of available time on recovery action performance. Having sufficient time will result in more successful recovery actions. According to the results, it can be inferred that available time has a significant effect on failure scenarios and their probabilities. As available time increases, operators have enough time to efficiently diagnose, make a decision and take action. As a result, human error is much lower in comparison with situations under limited available time.

4.2.3. Sensitivity analysis on input parameters

In this section, the sensitivity analysis on input parameters including available time, power level, and an operator's characteristics is performed. Fig. 9 presents the variation of the overall probability of the DP shuttle tanker collision as a function of input parameters. As can be seen on the horizontal axis of the figure, input parameters are scaled to a value between zero and one in order to be comparable.

As can be seen, available time has the greatest effect on collision probability. As presented in [8], available time refers to the amount of time that an operator has to diagnose and act upon an abnormal event. A shortage of time can affect the operator's ability to think clearly and consider alternatives. It may also affect the operator's ability to perform. Therefore, with limited available time, the collision probability is much higher.

After available time, an operator's fitness for duty has a significant effect on collision probability. Fitness for duty refers to whether or not the individual performing the task is physically and mentally fit to perform the task at the time. Factors that may affect fitness include fatigue, sickness, drug use (legal or illegal), overconfidence, personal problems, and distractions [8]. These characteristics affect the performance and the accuracy of the operator in making a diagnosis, making decisions and taking actions. Consequently, altering this factor significantly affects collision probability.

In addition, power level has a noteworthy impact on collision probability, as the main cause of the failure of this incident is lack of power. Changing the power level means that power returns to the system after the incident.

5. Application 2: loss of position of a DP shuttle tanker on August 5, 2007

5.1. Incident summary and failure scenario generation

On August 5, 2007, all of the position reference systems of a shuttle tanker were lost. Action was taken and the vessel was manually controlled by the DP operator. The vessel was kept steadily close to the ideal position/distance from a floating production storage and offloading (FPSO) unit. To safeguard the situation, emergency shutdown was activated. According to the investigation report, the vessel had not exceeded the maximum operation distance limit when emergency shutdown was activated.

The loading operation was stopped for 30 min while the DP system was taken to standby mode to rebuild the model and to allow the position reference system to be reset. Subsequently, all systems were found to be stable before the vessel was put back in DP mode.

When emergency shutdown was activated, the vessel communicated

Table 4
Failure events of the DESD presented in Fig. 2.

Dynamic event sequence diagram layers					
Detection	Diagnosis		Decision making and execution		
Failed to detect position and speed direction	Propulsion failure Reference failure Computer failure	Failed to drift off/drive off/ potential incidents diagnosis	Failed auto DC Failed manual DC	Failure of one or more recovery actions presented in Table 3	Failure of automatic keep position
Failed to detect alarm	Power failure Human error		Failure of automatic keep position		Failure of manual keep position
Failed to perform other visual detection	Bad environmental conditions Failed to control situation		Failure of manual keep position		

Table 5
More probable failure scenarios of the DP shuttle tanker collision.

Probability	Detection	Diagnosis	Decision making and execution		
5.53E-01	Alarm detected	Failure in control situation			
1.09E-01	Alarm detected	Control situation performed perfectly	Failed auto DC *		
6.38E-02	Alarm detected	Control situation performed perfectly	Failed manual DC**		
1.24E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard	
1.24E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator	
2.85E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of manual keep position
2.85E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of manual keep position
1.66E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of automatic keep position
1.66E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of automatic keep position
1.25E-06	Alarm detected	Control situation performed perfectly	Manual DC	Failure of tuning software	

* Automatic disconnection.
** Manual disconnection.

with the FPSO unit and informed it that all position reference systems had been lost. The FPSO asked when the vessel was ready to resume cargo operations. Once the systems had been recalibrated, reset and deemed stable and the vessel was put back in DP mode, the master adjudged that loading could be resumed under the current conditions and under the close monitoring of the DP systems. After having informed the FPSO accordingly, and in agreement with the FPSO, loading operations was resumed [41]. The sequence of events is highlighted in the dynamic event sequence diagram illustrated in Fig. 10.

Table 6
More probable failure scenarios of the DP shuttle tanker collision, assuming the reference system was faulty.

Probability	Detection	Diagnosis	Decision making and execution	
5.53E-01	Alarm detected	Failure in control situation		
1.09E-01	Alarm detected	Control situation performed perfectly	Failed auto DC*	
6.38E-02	Alarm detected	Control situation performed perfectly	Failed manual DC**	
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure of change position reference
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to recalibrate reference origin
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to deselect faulty sensor
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure of reference system recovery
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure of tuning software
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator
3.62E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard

* Automatic disconnection.
** Manual disconnection.

In order to model this incident based on the proposed methodology, the following inputs are considered.

- Reference systems are lost.
- The operator has enough fitness for duty and training, and the stress level is normal.
- Environmental conditions including wind and waves (force and directions) are in normal conditions.
- Propulsion and computer systems work properly.

The most probable failure scenarios, with considering the above-mentioned inputs, are presented in Table 8, and the overall failure

Table 7
More probable failure scenarios of the DP shuttle tanker collision, assuming sufficient time is available.

Probability	Detection	Diagnosis	Decision making and execution		
2.43E-01	Alarm detected	Control situation performed perfectly	Failed auto DC *		
1.42E-01	Alarm detected	Control situation performed perfectly	Failed manual DC**		
1.97E-02	Alarm detected	Failure in control situation			
1.39E-02	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of manual keep position
1.39E-02	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of manual keep position
8.10E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of automatic keep position
8.10E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of automatic keep position
9.69E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator	
9.69E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard	
1.41E-04	Alarm detected	Control situation performed perfectly	Manual DC	Tuning software	Failure of manual keep position

* Automatic disconnection.
** Manual disconnection.

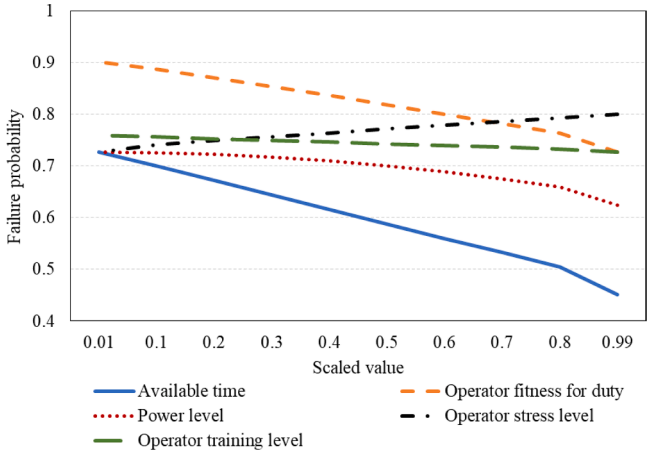

Fig. 9. Sensitivity analysis on input parameters for the DP shuttle tanker collision case.

probability is equal to 0.442.

According to the table, disconnection is performed in almost all of the most probable scenarios. This is mainly because of the failure of the reference systems. In such situations, it is more likely that the operator performs disconnection rather than trying to keep position. Furthermore, the failure probability of automatic disconnection is higher in comparison with automatic mode due to the faulty reference system. As the reference system has failed, accurate data cannot be transferred to the DP system. As a result, the computer and control system receive faulty data and the probability of failure increases. In manual mode, some of the faulty data would be modified by an operator's visual detections, and the probability of failure would be lower. However, after performing recovery action, DP components including the reference system return to work. Therefore, the failure probability of manual keep position is higher than automatic mode.

5.2. Sensitivity analysis

In the following sub-sections, the operation and environmental conditions at the time of the incident are changed to evaluate their impact on the most probable failure scenarios and system failure probability.

5.2.1. Available redundant system

DP systems rely on more than one position monitoring systems in order to obtain an accurate and reliable input for the current position of the vessel. For DP Class 2 or Class 3, it is necessary to use three different position monitoring systems. Two systems are insufficient, because if one system malfunctions and fails to give correct data, the DP control system is unable to identify which system is wrong. Thus, it is necessary to have at least three reference systems active to provide a two-out-of-three voting and identify the wrong set of data [42]. In the investigation report, it is assumed that all three reference systems are missed. In this section, it is assumed that there are other redundant systems that might be used as reference systems by operators. Table 9 presents the most probable scenarios in this situation.

The overall failure probability in this scenario decreases slightly to 0.441. The main difference of the most probable scenarios in this situation is that the operator tries to keep position and does not perform disconnection. The reason is that in the main case, all reference systems are lost, and the operator has to perform disconnection; but with a redundant reference system, the operator tries to maintain the vessel's position. In addition, keeping position is performed manually, as automatic mode is not reliable enough due to the lack of reference system.

5.2.2. Sensitivity analysis on input parameters

The overall failure probabilities of the DP system as a function of available time, power level and the operator's characteristics are presented in Fig. 11.

As can be seen in Fig. 11, available time has the greatest impact on failure probability, followed by the operator's characteristics and the power level. Changing the power level has the smallest effect on system failure probability, as the main cause of failure – the failure of the reference system – will remain through changing the power level.

6. Application 3: collision between a supply ship and an oil field on June 7, 2019

6.1. Incident summary and failure scenario generation

On June 7, 2019, a collision occurred between a supply ship and an oil field during loading/discharging. In this accident, a technical fault caused the vessel's load reduction mode to be activated, reducing the power to all of its thrusters to 10–15% of the maximum. Later, power was lost to two out of three bow thrusters. Its position was thereby lost. The officer attempted to switch the vessel to partly manual positioning.

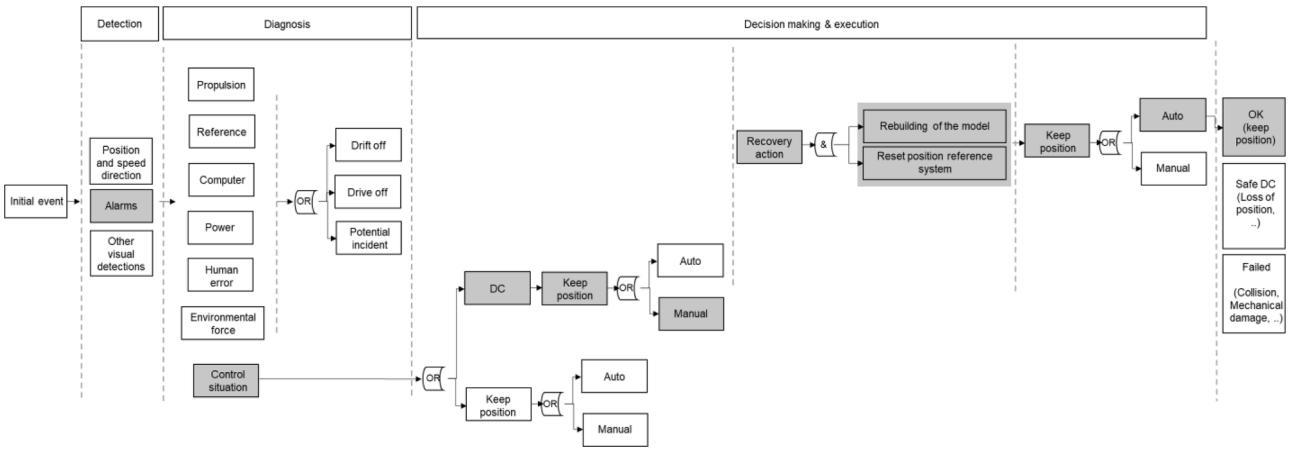

Fig. 10. Event sequence diagram of loss of position of the DP shuttle tanker.

Table 8
More probable failure scenarios of loss of position of the DP shuttle tanker.

Probability	Detection	Diagnosis	Decision making and execution		
2.40E-01	Alarm detected	Control situation performed perfectly	Failed auto DC *		
1.42E-01	Alarm detected	Control situation performed perfectly	Failed manual DC**		
1.97E-02	Alarm detected	Failure in control situation			
6.32E-03	Alarm detected	Control situation performed perfectly	Manual DC	Reference system recovery	Failure of manual keep position
6.32E-03	Alarm detected	Control situation performed perfectly	Manual DC	Deselect faulty sensor	Failure of manual keep position
6.32E-03	Alarm detected	Control situation performed perfectly	Manual DC	Recalibrate reference origin	Failure of manual keep position
6.32E-03	Alarm detected	Control situation performed perfectly	Manual DC	Change position reference	Failure of manual keep position
3.19E-03	Alarm detected	Control situation performed perfectly	Manual DC	Tuning software	Failure of manual keep position
1.91E-03	Alarm detected	Control situation performed perfectly	Manual DC	Deselect faulty sensor	Failure of automatic keep position
1.91E-03	Alarm detected	Control situation performed perfectly	Manual DC	Recalibrate reference origin	Failure of automatic keep position

* Automatic disconnection.
** Manual disconnection.

The vessel drifted against the facility, suffering extensive damage to the mast and equipment above the bridge, and denting its starboard side aft. Moreover, the mast caused damage to the oil field's lifeboat station. The master switched from DP to manual positioning. The programmable logic controller (PLC) was then reset to blackout safety system generators 2 and 4.

The direct causes of the incident were drifting as a result of inadequate thruster power, and the location of the loading/discharge operation on the windward (weather) side. The underlying causes that resulted in insufficient thruster power were related to the failure of or the incorrect installation of the equipment components, with disruption from the defective components leading to network failure in the blackout safety system ("network storm"), a loss of network frequency measurement on the main switchboard, activation of the load-reduction mode, and restriction of all thrusters to 10–15% of maximum output, nonconformity between DP commands and nominal input speed (rpm) feedback from all thrusters, and automatic shutdown of thrusters 1 and 3 [43]. The sequence of the incident events is highlighted in the dynamic event sequence diagram, illustrated in Fig. 12.

According to the investigation report, the initial event and conditions of this accident were as follows.

- The operator had enough fitness for duty and training, and the stress level was normal.
- There was not enough time and the vessel was in an emergency situation.
- Power was reduced to 15%.
- The reference and computer systems worked properly.
- The propulsion system including thrusters were not working properly.

These conditions are utilized here as model inputs, and failure scenarios are generated as results. Table 10 presents the most probable failure scenarios of the supply ship.

The overall failure probability is equal to 0.724. As can be seen, the scenario that occurred and is presented in the investigation report is the third most probable scenario among 271 possibilities. In addition, according to the second and third most probable scenarios, automatic disconnection is more likely to fail than manual. This matter can be inferred from the rest of the scenarios, as most of the successful disconnections are performed manually. This is mainly because DP components (power system, thrusters, etc.) do not work properly. As a result, the failure probability of automatic mode is higher. However, after performing recovery actions, DP components work properly. Therefore, manual keep positions are more likely to fail than automatic mode, as presented in the table.

6.2. Sensitivity analysis

As mentioned, operation and environmental conditions affect the collision probability of a supply ship. Sensitivity analysis on these parameters are performed in the following sub-sections.

Table 9
More probable failure scenarios of loss of position of a DP shuttle tanker, assuming DP vessel has a redundant reference system.

Probability	Detection	Diagnosis	Decision making and execution		
2.38E-01	Alarm detected	Control situation performed perfectly	Failure of automatic keep position		
1.40E-01	Alarm detected	Control situation performed perfectly	Failure of manual keep position		
1.97E-02	Alarm detected	Failure in control situation			
6.25E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Change position reference	Failure of manual keep position
6.25E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Recalibrate reference origin	Failure of manual keep position
6.25E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Deselect faulty sensor	Failure of manual keep position
6.25E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Reference system recovery	Failure of manual keep position
3.16E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Tuning software	Failure of manual keep position
2.40E-03	Alarm detected	Control situation performed perfectly	Failed auto DC*	Reference system recovery	Failure of automatic keep position
1.89E-03	Alarm detected	Control situation performed perfectly	Manual keep position	Reference system recovery	Failure of automatic keep position

* Automatic disconnection.

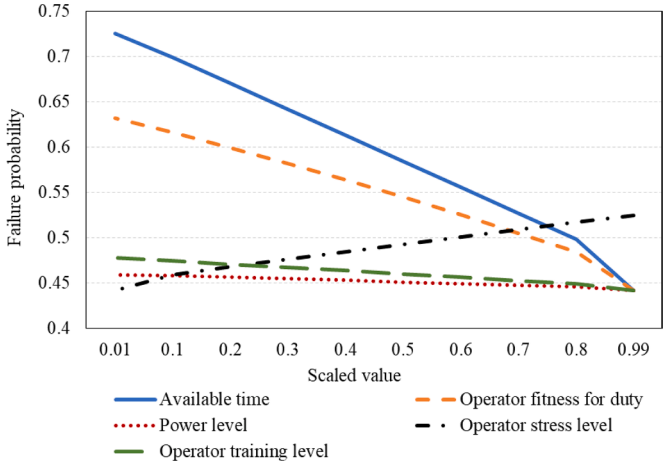

Fig. 11. Sensitivity analysis on input parameters for the DP shuttle tanker loss of position case.

6.2.1. *Poor fitness for duty and high stress level of operator*

In the investigation report, there is no information regarding the operator's fitness for duty and stress level. In the main case study, it is assumed that the operator's fitness for duty and stress level fall within a normal range, and the results are presented in Table 10 accordingly. However, in this section, it is assumed that the level of the operator's fitness for duty is low and the stress level is high.

According to the PetroHRA [8], the performance of operators with poor fitness for duty is negatively affected by the work processes at the facility (e.g., shift turnover does not include adequate communication about ongoing maintenance activities; poor command and control by supervisor(s); performance expectations are not made clear). In addition, a high stress level is defined by PetroHRA as a level of stress greater than the nominal level (e.g., multiple instruments and annunciators sound unexpectedly and at the same time; loud, continuous noise compromises ability to focus attention on the task; the consequences of the task represent a threat to facility safety) [8]. Table 11 presents the most probable failure scenario of the supply ship operated by an operator with poor fitness for duty and high stress level.

The overall failure probability of this case increases significantly from 0.724 to 0.827. The most probable scenarios remain almost the same. However, more recovery actions tend to fail due to the higher probability of human errors.

6.2.2. *Sufficient time and an operator with poor fitness for duty and high stress level*

In this section, it is assumed that the operator has poor fitness for duty and a high stress level, just as in the previous section. However, in this scenario it is assumed that there is sufficient time for the operator to diagnose, make a decision and take action. Table 12 presents the most probable failure scenarios.

The overall failure probability of this case drops to 0.556. The results show that more recovery actions are performed in comparison to the previous section's results due to sufficient available time. However, the recovery actions tend to fail due to low human reliability.

6.2.3. *Sensitivity analysis on input parameters*

The overall collision probability of the supply ship as a function of available time, power level and the operator's characteristics are presented in Fig. 13.

As can be seen, the collision probabilities have the same trend as the

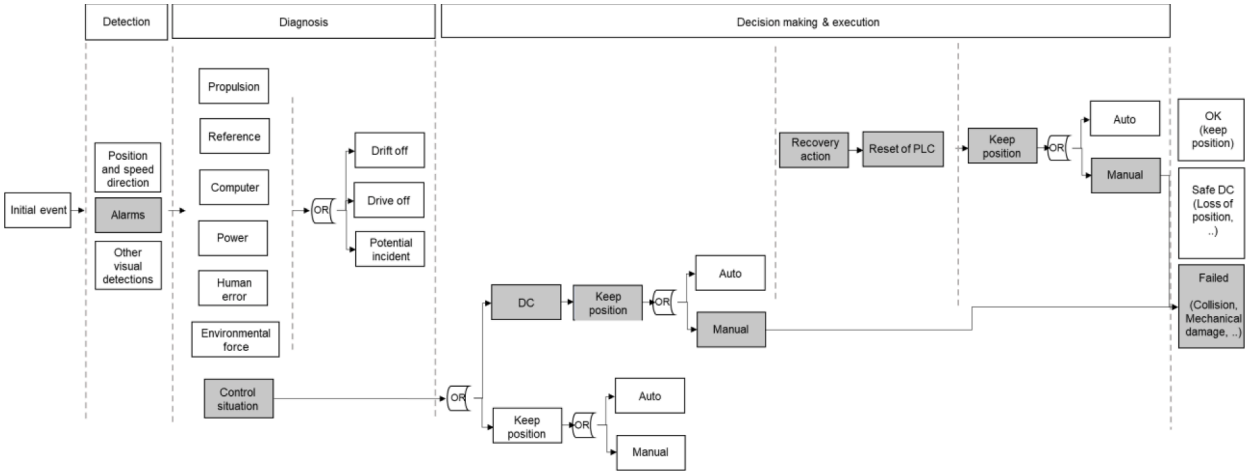

Fig. 12. Event sequence diagram of the supply ship collision.

Table 10
More probable failure scenarios of the supply ship collision.

Probability	Detection	Diagnosis	Decision making and execution		
5.53E-01	Alarm detected	Failure in control situation			
1.07E-01	Alarm detected	Control situation performed perfectly	Failed automatic DC *		
6.38E-02	Alarm detected	Control situation performed perfectly	Failed manual DC**		
1.23E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator	
1.23E-04	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard	
2.84E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of manual keep position
2.84E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of manual keep position
1.42E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of automatic keep position
1.42E-05	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of automatic keep position
6.41E-06	Alarm detected	Control situation performed perfectly	Automatic DC	Failure to start equipment on alternative switchboard	

* Automatic disconnection.
** Manual disconnection.

probabilities presented for the DP shuttle tanker accident on November 13, 2006, as the main cause of failure of both was low power level.

7. Results summary

As presented in the previous sections, system failure probability is strongly affected by the operation and environmental conditions at the time of the incident. According to these results, it can be inferred that this dependency varies case by case and is contingent on the nature of the incident. For instance, the failure probability of case 2 is more strongly affected by human characteristics in comparison to cases 1 and 3. As can be inferred from the figures, operator fitness for duty and operator stress level change more in case 2 (Fig. 11) in comparison to cases 1 (Fig. 9) and 3 (Fig. 13).

In this section, a comparison between the sensitivity of failure probabilities to input parameters for the three case studies has been performed. Table 13 presents the variation of failure probability by changing the input parameters from zero to one for all three case studies. Zero and one present the worse and best-case statuses of the input parameters. For instance, the available time input changes from no time (zero) to adequate (one) available time; or the operator's stress level changes from no stress (zero) to high stress level (one). As can be seen, changing stress level from zero to one has a negative effect on failure probability reduction (−0.07, −0.08, −0.07) ,[2] i.e., by increasing stress level of operators the probability of system failure exacerbates. The main reason is that human error rises with increasing stress level and results in higher system failure probability.

Another important point that could be inferred from Table 13 is that the percentage values presented for case 2 (64.24%, 42.94%, −18.61%, 8.04%, 3.92%)[3] are higher due to the lower system failure value in comparison to cases 1 (37.90%, 24.10%, −10.07%, 4.42%, 14.05%)[4] and case 3 (38.42%, 24.37%, −10.19%, 4.46%, 14.10%)[4].

As indicated in Table 13, available time is the most important factor in all cases (has the highest value), followed by the operator's fitness for duty, stress and training level. It is demonstrated that power level has a greater impact on probability in cases 1 (14.05%) and case 3 (14.10%) in comparison to case 2 (3.92%). The reason is that the main cause of failure in cases 1 and 3 is a lack or low level of power. Therefore, changing the power level will help the system to return to work. However, in case 2, the main reason for failure is the reference system, so changing the power level will not recover the faulty reference system, hence the main cause of failure will remain.

Available time has almost the same effect across the three cases with a reduction of failure probability equals to 0.28. The reason is that in all three cases, a component is failed (in cases 1 and 3, the power system; in case 2, the reference system), and the operator try to maintain position and perform recovery actions within the available time. Changing available time affect human related events in the dynamic event sequence diagram, such as "operator control situation" or "recovery actions", which are the same for these three cases.

The small difference between values in fitness for duty (0.18, 0.19, 0.18) ,[4] stress (−0.07, −0.08, −0.07)[5], and training level (0.03, 0.04, 0.03)[5] across the three cases owes to the difference between the effects of human error on the reference and power system failures. According to the IMCA reports [31], the probability of human error in power systems is higher than in reference systems. As a result, human factors have a greater impact on power system failure probability than reference system failure probability. In cases 1 and 3, the power system is failed. Human errors affect working components including reference system. In case 2, the reference system failed, and human errors affect the power system. Changing human characteristics has a slightly greater impact on case 2 (0.19, −0.08, 0.04)[6], as it may affect the failure probability of the power system. However, this effect is lower in cases 1 (0.18, −0.07, 0.03)[5] and case 3 (0.18, −0.07, 0.03)[6], as human characteristics affect the failure probability of the reference system. Another reason for the slightly greater effect of human characteristics in case 2 may owe to there being sufficient available time in this case. As presented in Section 5, in case 2, operators have enough time to diagnose, make a decision and take action. As a result, their impact on the failure probability of the system is higher than in cases 1 and 3 where there is limited available time.

[2] For Case 1, 2, and 3.
[3] For available time, operator's fitness for duty, stress level, training level, and power level, respectively.
[4] For cases 1, 2, and 3, respectively.
[5] For operator's fitness for duty, stress level, and training level, respectively.

Table 11
More probable failure scenarios of the supply ship collision, assuming operator has poor fitness for duty and high stress level.

Probability	Detection	Diagnosis	Decision making and execution		
7.04E-01	Alarm detected	Failure in control situation			
7.00E-02	Alarm detected	Control situation performed perfectly	Failed auto DC *		
5.27E-02	Alarm detected	Control situation performed perfectly	Failed manual DC**		
6.51E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator	
6.51E-05	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard	
9.75E-06	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of manual keep position
9.75E-06	Alarm detected	Control situation performed perfectly	Manual DC	Start of equipment on alternative switchboard	Failure of manual keep position
5.34E-06	Alarm detected	Control situation performed perfectly	Auto DC	Failure to start new generator	
5.34E-06	Alarm detected	Control situation performed perfectly	Auto DC	Failure to start equipment on alternative switchboard	
3.88E-06	Alarm detected	Control situation performed perfectly	Manual DC	Start equipment on alternative switchboard	Failure of automatic keep position

* Automatic disconnection.
** Manual disconnection.

8. Discussion

8.1. Method effectiveness

In this study, the application of a new supervised dynamic probabilistic risk assessment model has been examined and discussed. In this model, knowledge of the system is explicitly used in an optimization model to predict possible failure scenarios. In the optimization model, a supervised learning algorithm is used to find the optimal solution, which is the desired failure scenario, i.e., instead of focusing on obtaining all possible scenarios, we have approached the problem of exploring the desired failure scenarios efficiently.

The model has been applied to solve DPRA problems in three different DP accidents. The accidents' characteristics have been explored using the investigation reports of each accident, and the model outputs have been compared with the failure scenarios presented in these investigation reports. According to these comparisons, the proposed model can predict the most probable failure scenarios with a high degree of accuracy. In addition, the execution time of the model is under 1 min to generate 271 failure scenarios, which is significantly lower than other conventional DPRA methods presented in the literature. In the accompanying article (Part 1) [19], a comparison between the execution time of a conventional DPRA (dynamic ESD) and the supervised (optimization based) DPRA methods is performed. These two methods are applied to a case study, and execution times at different time intervals are recorded. Results show that the execution time of the supervised DPRA method is significantly lower than the conventional DPRA method.

8.2. Model validation and sensitivity analysis

Model validation and sensitivity analysis have been employed to assess the correctness of the model specification and to analyze the strength of the conclusions drawn. The model has been validated using three different DP accidents. Input data have been derived from the investigation reports of accidents, and outputs (possible failure scenarios) have been generated using the proposed model. In cases 1 and 3, the real accident has been identified among the top three most probable failure scenarios generated by the model. The second and third most probable failure scenarios for case 1 (Table 5) and 3 (Table 10), respectively, are the real failure scenarios as presented in the investigation report.

In addition, a sensitivity analysis on input parameters has been performed for all three case studies. The results of the sensitivity analysis are particularly useful in gaining confidence in the results of the primary analysis, and are important in situations where a model is likely to be used in a future investigation.

8.3. Operation and environmental conditions

The simulation results have demonstrated that accident scenarios are highly dependent on system dynamics, hence the event sequences need to be analyzed with great care. In particular, it has been shown that operation and environmental conditions' impacts on a system's risk level are contingent on the nature of the accident. For instance, power level had a smaller effect on case 2 (changes from 0.46 to 0.44 as presented in Fig. 11) where the reference system was the main cause of failure, as having more power does not necessarily help the reference system to return to operation. However, power level had a greater effect on case 1 (changes from 0.71 to 0.61 as presented in Fig. 9) and case 3 (changes from 0.71 to 0.61 as presented in Fig. 13) where the main cause of the accident was a blackout.

Such findings illustrate the importance of a comprehensive and accurate diagnosis at the early stage of initial event (incident) detection. Knowing the main cause helps to determine the critical affecting parameters, so that one can try to keep these within an acceptable range to prevent the negative consequences from being exacerbated.

8.4. Human and organizational factors

Modeling human and organizational factors plays a very important role in DP system risk analysis. In order to model a system with high accuracy – particularly in emergency situations – the human and components model must be integrated into the DPRA work. In this study, the SPAR-H method has been used to include human and organizational factors. The factors considered here were the operator's fitness for duty, stress and training level. With improvements in human modeling, the integrated DPRA methodology introduced here can become even more powerful.

8.5. Future works

According to the sensitivity analysis results, available time has the greatest effect on the risk level of a DP system operation in emergency situations. Therefore, managing the available time may significantly reduce the risk level of the system. Fault diagnosis models may provide useful information to operators by analyzing and interpreting available

Table 12
More probable failure scenarios of the supply ship collision, assuming there is sufficient time and the operator has low fitness for duty and high stress level.

Probability	Detection	Diagnosis	Decision making and execution		
2.01E-01	Alarm detected	Control situation performed perfectly	Failed automatic DC *		
1.70E-01	Alarm detected	Failure in control situation			
1.51E-01	Alarm detected	Control situation performed perfectly	Failed manual DC**		
7.92E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of manual keep position
7.92E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start equipment on alternative switchboard	Failure of manual keep position
4.47E-03	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start new generator	
4.47E-03	Alarm detected	Control situation performed perfectly	Manual DC	Failure to start equipment on alternative switchboard	
3.15E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start new generator	Failure of automatic keep position
3.15E-03	Alarm detected	Control situation performed perfectly	Manual DC	Start equipment on alternative switchboard	Failure of automatic keep position
6.49E-04	Alarm detected	Control situation performed perfectly	Auto DC	Start equipment on alternative switchboard	Failure of manual keep position

* Automatic disconnection.
** Manual disconnection.

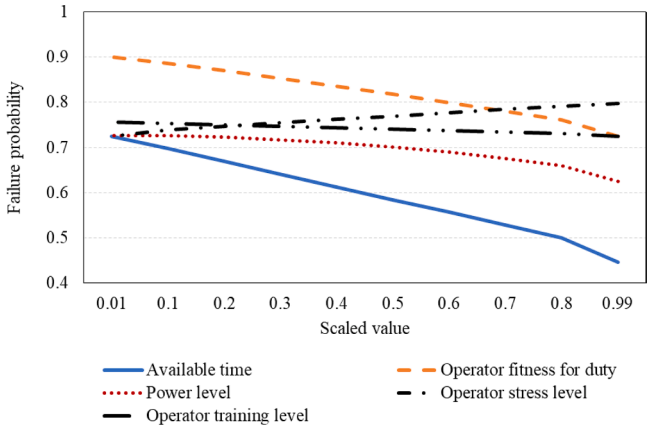

Fig. 13. Sensitivity analysis on input parameters for the supply ship collision case.

data. With the development of artificial intelligence (AI), many new methods have been introduced to research into the fault diagnosis of complex systems. Utilizing these methods in DP systems enables operators to determine the root cause of failure, and consequently to significantly reduce the time required for the diagnosis phase.

In addition, prediction models may help operators to make a better decision within a limited timeframe. In emergency situations, there are multiple alternative decision scenarios that can be made to control the hazard. Prediction models could be employed to simulate each decision scenario and achieve a better picture of their consequences. Fault diagnosis methods and prediction models for DP systems should be explored in future works to help operators to make better decisions in emergency situations.

9. Conclusion

In this paper, the capabilities of supervised dynamic probabilistic risk assessment methodology to evaluate the risk level of dynamic positioning systems in emergencies have been demonstrated. The supervised dynamic PRA methodology has been applied to a DP system to enable a more efficient and yet accurate evaluation of the risk level of the system during emergencies, as shown through an analysis of the case studies presented.

Table 13
Reduction of DP system failure probability by changing input parameters from 0 to 1.

Parameter	Reduction of failure probability (percentage)		
	Case 1	Case 2	Case 3
Available time 0: No time 1: Adequate time	0.28 (37.90%)	0.28 (64.24%)	0.28 (38.42%)
Operator's fitness for duty 0: No fitness 1: High level of fitness	0.18 (24.10%)	0.19 (42.94%)	0.18 (24.37%)
Operator's stress level 0: No stress 1: High stress level	−0.07 (−10.07%)	−0.08 (−18.61%)	−0.07 (−10.19%)
Operator's training level 0: No training 1: High level of training	0.03 (4.42%)	0.04 (8.04%)	0.03 (4.46%)
Power level 0: Blackout 1: Full power available	0.10 (14.05%)	0.02 (3.92%)	0.10 (14.10%)

These cases were three DP system incidents that have occurred in the Norwegian offshore sector. The information required to perform modeling has been gathered from the available investigation reports for each incident. The model outputs are the most probable scenarios and risk levels of the system after each incident. Comparing these results with the investigation reports has revealed that the model has a high level of accuracy, as the accidents are sorted among predicted high probable failure scenarios. Moreover, sensitivity analysis on the input parameters of the model has been performed, with the results indicating that available time has the greatest impact on the risk level. As a result, having an efficient predictive risk model could reduce the risk level of the system by providing useful information to operators so that they can make a decision within a shorter timeframe.

CRediT authorship contribution statement

Tarannom Parhizkar: Conceptualization, Formal analysis, Validation, Data curation, Writing - original draft. **Ingrid Bouwer Utne:**

Conceptualization, Writing - review & editing, Supervision. **Jan Erik Vinnem:** Conceptualization, Writing - review & editing, Supervision. **Ali Mosleh:** Conceptualization, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Værnø SA, Skjetne R, Kjerstad ØK, Calabrò V. Comparison of control design models and observers for dynamic positioning of surface vessels. Control Eng Pract 2019; 85:235–45.
[2] Ahani A, Ketabdari MJ. Alternative approach for dynamic-positioning thrust allocation using linear pseudo-inverse model. Appl Ocean Res 2019;90:101854.
[3] Lloyd G. Rules for classification and construction, I-Part 1. Anal Tech 1998:43–6.
[4] Vedachalam N, Ramadass GA. Reliability assessment of multi-megawatt capacity offshore dynamic positioning systems. Appl Ocean Res 2017;63:251–61.
[5] Chen H, Moan T, Verhoeven H. Safety of dynamic positioning operations on mobile offshore drilling units. Reliab Eng Syst Saf 2008;93(7):1072–90.
[6] Dong Y, Vinnem JE, Utne IB. Improving safety of DP operations: learning from accidents and incidents during offshore loading operations. EURO J Decis Process 2017;5(1–4):5–40.
[7] Dong Y, Rokseth B, Vinnem JE, Utne IB. Analysis of dynamic positioning system accidents and incidents with emphasis on root causes and barrier failures. In: Proceedings of ESREL 2016 (Glasgow, Scotland, 25-29 September 2016); 2016. p. 166.
[8] Bye, A., Laumann, K., Taylor, C., Rasmussen, M., Øie, S., van de Merwe, K., ... & Massaiu, S. (2017). The petro-HRA guideline.
[9] Dong Y, Vinnem JE, Utne IB. Towards an online risk model for dynamic positioning operations. In: Safety and Reliability-Safe Societies in a Changing World, Proceedings of ESREL 2018, June 17-21, 2018; 2018.
[10] Hogenboom S, Rokseth B, Vinnem JE, Utne IB. Human reliability and the impact of control function allocation in the design of dynamic positioning systems. Reliab Eng Syst Saf 2020;194:106340.
[11] Parhizkar T, Aramoun F, Saboohi Y. Efficient health monitoring of buildings using failure modes and effects analysis case study: air handling unit system. J Build Eng 2020;29:101113.
[12] Parhizkar T, Aramoun F, Esbati S, Saboohi Y. Efficient performance monitoring of building central heating system using Bayesian Network method. J Build Eng 2019; 26:100835.
[13] Chang YHJ, Mosleh A. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: part 1: overview of the IDAC Model. Reliab Eng Syst Saf 2007;92(8):997–1013.
[14] Hsueh KS, Mosleh A. The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. Reliab Eng Syst Saf 1996;52(3):297–314.
[15] Chang YHJ, Mosleh A. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: part 1: overview of the IDAC Model. Reliab Eng Syst Saf 2007;92(8):997–1013.
[16] Parhizkar T, Hogenboom S, Vinnem JE, Utne IB. Data driven approach to risk management and decision support for dynamic positioning systems. Reliab Eng Syst Saf 2020;201:106964.
[17] Hu, Y. (2005). A guided simulation methodology for dynamic probabilistic risk assessment of complex systems (Doctoral dissertation).
[18] Nejad-Hosseinian, S.H. (2007). Automatic generation of generalized event sequence diagrams for guiding simulation based dynamic probabilistic risk assessment of complex systems (Doctoral dissertation).
[19] Parhizkar T, Balali S, Mosleh A. An entropy based bayesian network framework for system health monitoring. Entropy 2018;20(6):416.
[20] Parhizkar T, Vinnem JE, Utne I, Mosleh A. Supervised dynamic probabilistic risk assessment of complex systems, part 1: general overview. Reliab Eng Syst Saf 2020. Submitted.
[21] Calafiore GC, El Ghaoui L. Optimization models. Cambridge University Press; 2014.
[22] Sarker RA, Newton CS. Optimization modelling: a practical approach. CRC Press; 2007.
[23] Herdzik J. Dynamic positioning systems during emergency or unexpected situations. J KONES 2013;20(3):153–9.
[24] Faÿ H. Dynamic positioning systems: principles, design, and applications 1990.
[25] Swaminathan S, Smidts C. The mathematical formulation for the event sequence diagram framework. Reliab Eng Syst Saf 1999;65(2):103–18.
[26] Hu Y, Luo PC. Event sequence diagram based safety critical event identification and sensitive analysis. Future communication, computing, control and management. Berlin, Heidelberg: Springer; 2012. p. 157–62.
[27] Khan F, Rathnayaka S, Ahmed S. Methods and models in process safety and risk management: past, present and future. Process Saf Environ Prot 2015;98:116–47.
[28] Swaminathan S, Smidts C. The event sequence diagram framework for dynamic probabilistic risk assessment. Reliab Eng Syst Saf 1999;63(1):73–90.
[29] Acosta C, Siu NO. Dynamic event tree analysis method (DETAM) for accident sequence analysis, 1991. Cambridge, Mass.: Dept. of Nuclear Engineering, Massachusetts Institute of Technology; 1991.
[30] Acosta CG, Siu NO. Dynamic event tree analysis method (DETAM) for accident sequence analysis. In: Massachusetts Institute of Technology, Nuclear Engineering Department, MITNE-295; 1991.
[31] The International Marine Contractors Association. dynamic positioning station keeping review, incidents and events reported for (2004-2015). International Marine Contractors Assosiation; 2005–17.
[32] Cruz DF, Fonseca DDR. WSOG and Emergency Disconnection Guidelines. In: OTC Brasil. Offshore Technology Conference; 2017.
[33] Parhizkar T, Vinnem JE, Utne IB. Dynamic probabilistic safety assessment framework to assist decision-making in complex systems, case study: dynamic positioning drilling unit. Risk Anal 2019. Submitted.
[34] Rokseth B, Skjong S, Pedersen E. Modeling of generic offshore vessel in crane operations with focus on strong rigid body connections. IEEE J Oceanic Eng 2016; 42(4):846–68.
[35] Chen H, Moan T, Verhoeven H. Safety of dynamic positioning operations on mobile offshore drilling units. Reliab Eng Syst Saf 2008;93(7):1072–90.
[36] Zhang, W. (2015). Dynamic Modelling, Simulation and Visualization of Marine Crane Operations on DP Vessels (Master's thesis, NTNU).
[37] Lee J, Leyffer S, editors. Mixed integer nonlinear programming (Vol. 154). Springer Science & Business Media; 2011.
[38] dos Santos Coelho L. An efficient particle swarm approach for mixed-integer programming in reliability–redundancy optimization applications. Reliab Eng Syst Saf 2009;94(4):830–7.
[39] Members/NBN, Team. Significant incident investigation xxx dp incident on xxx. Teekay Shipping (Canada) Ltd.; 2006.
[40] Sørensen AJ. A survey of dynamic positioning control systems. Annu Rev Control 2011;35(1):123–36.
[41] Lund T. Incident investigation, loss of DP at XXX. TeekayMarine; 2007.
[42] Specht C, Pawelski J, Smolarek L, Specht M, Dabrowski P. Assessment of the positioning accuracy of DGPS and EGNOS systems in the Bay of Gdansk using maritime dynamic measurements. J Navig 2019;72(3):575–87.
[43] Oplenskedal A, Bjørheim LS. Investigation of collision between Sjoborg supply ship and Statfjord A. Pet Saf Auth Norway 2019.